International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

Secure IoT Communication in Distributed Systems Using Adaptive Symmetric Key Encryption

1Prachi Prakashrao Deshpande [2]Gajanan Kishanrao Mangnale

Submitted:02/05/2024 **Revised**: 28/06/2024 **Accepted:** 06/07/2024

Abstract: The rapid proliferation of Internet of Things (IoT) devices in distributed systems has significantly enhanced connectivity and real-time data exchange across diverse applications such as smart cities, healthcare, and industrial automation. However, this widespread deployment introduces critical challenges related to data security, privacy, and efficient communication, particularly in resource-constrained and heterogeneous environments. Traditional encryption techniques often fail to meet the dynamic requirements of IoT systems due to their computational overhead and lack of adaptability. This paper proposes a novel approach for secure IoT communication in distributed systems using adaptive symmetric key encryption, which dynamically adjusts encryption parameters based on network conditions, device capabilities, and data sensitivity. The proposed system employs a lightweight symmetric encryption mechanism combined with an adaptive key generation and management strategy to ensure secure data transmission while minimizing computational and energy costs. The framework integrates real-time monitoring and intelligent decision-making to optimize encryption strength, thereby achieving a balance between security and performance. Furthermore, the system incorporates robust authentication protocols and secure key distribution techniques to prevent unauthorized access and mitigate common attacks such as replay attacks, man-in-the-middle attacks, and data tampering. Experimental evaluation demonstrates that the proposed approach significantly improves communication efficiency, reduces latency, and enhances overall system security compared to conventional methods. The results indicate that adaptive symmetric key encryption is a promising solution for securing communication in distributed IoT environments, offering scalability, flexibility, and resilience against evolving cyber threats. This work contributes toward the development of intelligent, secure, and efficient IoT communication frameworks for next-generation distributed systems.

Keywords: *IoT Security, Adaptive Encryption, Symmetric Key Cryptography, Distributed Systems, Secure Communication, Lightweight Encryption, Key Management, Data Privacy, Network Security, Smart Systems*

I. Introduction

Through the rapid development of the Internet of Things (IoT), the capacities of devices to communicate with one another, interact with one another, and share data across scattered networks have undergone a complete metamorphosis. This has resulted in a thorough transformation of the capabilities of devices. Through the capabilities of the Internet of Things, it is now possible to connect billions of intelligent objects in a seamless manner. The difficulty of this situation cannot be overstated. Each and every one of these gadgets, which comprise everything from sensors and wearable devices to industrial gear and smart home systems, are covered in this category. This ecosystem's seamless integration makes it possible to collect data in real time, the monitoring of that data, and the making of intelligent decisions based on that data. Consequently, it offers a significant contribution to applications such as smart cities, healthcare, agriculture, transportation, and industrial automation, among others. In addition to that, it is utilized in the commercial transportation industry. The ever-increasing quantity and complexity of

[1]*prachijoshi4478@gmail.com*
gajananmangnale@gmail.com

Lecturer Government Polytechnic, Hingoli, Lecturer Government Polytechnic, Nanded

Internet of Things networks, on the other hand, provide a number of significant issues. These challenges are particularly concerning with regard to the protection of data privacy, the preservation of secure communication, and the dependability of the system.

When devices are implemented in environments that are distributed for the Internet of Things, they typically operate in a range of settings that are limited in terms of the resources that they have available through those settings. When it comes to energy, memory, and processing power, these environments are defined by having limited resources to work with. The application of normal security methods, which are typically designed for high-performance computer systems, is made more difficult as a result of these limitations. High-performance computer systems are often the target audience for the development of these techniques. There are still a great number of Internet of Things systems that are susceptible to a wide range of cyber threats, such as eavesdropping, data tampering, replay attacks, and unauthorized access. This is a result of the fact that a significant percentage of these devices continue to be vulnerable to the dangers that have been described. As a consequence of this, ensuring secure communication in circumstances such as these is a crucial necessity for preserving the integrity of sensitive data and ensuring that it continues to be kept confidential.

When it comes to the process of ensuring the security of communications that take place through the Internet of Things (IoT), encryption is a vital component that must be included. The transformation of plaintext data into a format that cannot be read is the method that is used to achieve this goal. It is because of this that the data are safeguarded from being accessed by unauthorized parties. In Internet of Things (IoT) systems, symmetric key encryption is generally applied because it is less difficult, more effective, and takes fewer processing resources than asymmetric encryption methods. This is because symmetric key encryption works better than asymmetric encryption methods. symmetric key encryption is helpful in this regard since it eliminates the need for asymmetric encryption, which is a need for encrypted data. The conventional methods of symmetric encryption, on the other hand, often make use of static keys and encryption settings that are fixed. This leads one to believe that these methods might not be appropriate for systems that are both dynamic and scattered, such as those that are present in the Internet of Things (IoT). Static encryption methods render them vulnerable to the possibility of key compromise and do not provide the flexibility to respond to changing network conditions and threat levels. This leaves them vulnerable to the possibility of key compromise. Different types of encryption, including static encryption, are susceptible to key compromise, just like other types of encryption.

For the purpose of overcoming these limitations, the utilization of adaptive encryption algorithms is currently becoming an increasingly vital component. The capabilities of the device, the bandwidth of the network, the availability of energy, and the privacy of the data are some of the contextual factors that these mechanisms need to be able to take into consideration when making adjustments to their settings. These adjustments should be able to be made in a dynamic manner. A solution that has the potential to be advantageous is the development of adaptive symmetric key encryption. This is due to the fact that it allows for the changing of key sizes, encryption algorithms, and security levels in real time. The flexibility of the system not only improves the system's security, but it also improves the system's speed by lowering the amount of processing overhead that is not actually required. This is accomplished by reducing the amount of unnecessary overhead.

Managing keys in a secure manner is yet another fundamental problem that must be overcome in distributed systems. This challenge must be overcome. For the purpose of preventing unauthorized access and ensuring that the system can be scaled effectively, it is essential that the process of establishing, distributing, and upgrading encryption keys be conducted in a manner that is both efficient and secure. Moreover, it is of the utmost importance that the procedure be capable of being improved. When it comes to managing the huge number of devices and the dynamic interactions that take place in networks that are connected to the Internet of Things, typical key management solutions sometimes fail to meet the task. This is because the Internet of Things introduces new challenges. Adaptive encryption methods and intelligent key management procedures are an imperative necessity for establishing robust security in environments that are distributed. This is a requirement that cannot be avoided. The factors

that were discussed earlier are the explanation for this.

Additionally, the Internet of Things (IoT) has been combined with developing technologies such as cloud computing, edge computing, and artificial intelligence (AI), which has resulted in the opening of new opportunities for enhancing the system's efficiency and security. This has led to the creation of new possibilities. The incorporation of these technologies has contributed to the realization of certain capabilities, which were previously unattainable. An example of this would be how edge computing makes it possible to process data in a location that is physically closer to the point of origin of the data. Therefore, this results in a reduction in latency and an improvement in response time. Along the same lines, a number of technologies that come from the field of artificial intelligence can be utilized to identify irregularities, be able to anticipate potential threats in the future, and dynamically optimize encryption systems. The application of these innovations leads to the development of communication frameworks for the Internet of Things that are not only intelligent but also contain an exceptionally high level of security.

Despite the fact that these achievements have been made, there are still a great deal of obstacles in the field of research that need to be overcome. Because more robust encryption algorithms often result in higher computational and energy costs, one of the most important issues that must be addressed is to achieve a balance between security and performance. This is one of the fundamental challenges that must be overcome. Furthermore, it is required to design systems that are both durable and scalable in order to guarantee interoperability across a wide range of devices and to protect the integrity of data while it is being transported over remote networks. This is necessary in order to comply with the requirements of the Internet of Things (IoT). As a consequence of this, there is an unprecedented level of demand for encryption strategies that are not only lightweight but also versatile and effective within their application. For the first time in history, this requirement is more urgent than it has ever been. The purpose of this research is to develop a framework for secure communication that can be utilized by Internet of Things (IoT) devices that are located in different locations. This framework will be developed with the assistance of adaptive symmetric keyboard encryption. Taking into account the features of the system, this technique of encryption performs a dynamic update of the encryption parameters in real time. This modification is accomplished throughout the encryption process. Through the application of the strategy that has been described, there have been efforts made to improve data security while simultaneously reducing the amount of resources that are being consumed. As a result of this, it is suited for Internet of Things scenarios that involve a large number of devices that are communicating with one another and have a restricted amount of resources. The application of strategies for adaptive decision-making and efficient key management is what makes this system so effective. It ensures that scattered devices are able to communicate in a manner that is not only reliable and efficient, but also secure and reliable.

In conclusion, the growing utilization of technologies associated with the Internet of Things calls for the development of improved security solutions that are capable of resolving the specific issues that are brought about by the dispersion of systems. When it comes to the protection of communication between Internet of Things (IoT) devices, the adoption of the adaptive symmetric key encryption technique offers a mechanism that is not only adaptable but also very effective. In addition to this, it offers enhanced resistance against cyber threats while also preserving the system's current level of performance. A contribution is made by the findings of this research to the ongoing efforts that are being made to establish infrastructures for the Internet of Things that are intelligent, scalable, and safe for applications that will be developed in the future.

II. Literature Survey

Shivaramakrishna et. al. sattes that the rapid proliferation of cloud computing has necessitated advanced security mechanisms to safeguard sensitive data stored in remote servers. However, this paradigm shift has raised several security concerns, particularly safeguarding private information stored on faraway cloud servers. This study proposes a ground-breaking hybrid cryptographic framework for the secure data storage requirements of cloud computing. The framework incorporates time-limited access control, adaptive key management, and two strong encryption methods: RSA and Advanced Encryption Standard -

One Time Password (AES-OTP). AES-OTP and RSA provide symmetric and asymmetric encryption levels to improve data confidentiality and integrity. With the introduction of an intelligent framework for key creation, distribution, and rotation through the adaptive key management component, the security of cryptographic operations is gradually increased. Additionally, time-limited access control helps to protect data privacy by imposing rigorous temporal constraints on data access and reducing security flaws. The effectiveness of the suggested framework is confirmed by thorough performance assessments, which show astonishing accuracy, precision, recall, and F1-score values of 99.12%, 98.78%, 98.11%, and 98.56%. This demonstrates its outstanding skills in protecting private information from unauthorized access and guaranteeing its secrecy in cloud storage settings. [1]

Cheng et. al. states that Wireless sensor networks are usually applied in hostile areas where nodes can easily be monitored and captured by an adversary. Designing a key distribution scheme with high security and reliability, low hardware requirements, and moderate communication load is crucial for wireless sensor networks. To address the above objectives, we propose a new key distribution scheme based on an ECC asymmetric encryption algorithm. The two-way authentication mechanism in the proposed scheme not only prevents illegal nodes from accessing the network, but also prevents fake base stations from communicating with the nodes. The complete key distribution and key update methods ensure the security of session keys in both static and dynamic environments. The new key distribution scheme provides a significant performance improvement compared to the classical key distribution schemes for wireless sensor networks without sacrificing reliability. Simulation results show that the proposed new scheme reduces the communication load and key storage capacity, has significant advantages in terms of secure connectivity and attack resistance, and is fully applicable to wireless sensor networks. [2]

Mihaljevi´c et.al explains that considering the problem of data access control when the subscribers are IoT devices with initialization that cannot be updated during the entire life cycle. A generic framework and a particular instance for conditional data access control within IoT are proposed. The generic framework is based on the employment of a dedicated secret key-based broadcast encryption scheme where encrypted credentials for conditional data access is available in the blockchain and encrypted data subject to conditional access are available in an off-chain source of streaming data. Reduction of the keys management overhead in comparison with a straightforward decryption keys delivery is experimentally illustrated. An instance of the proposed framework built over the Ethereum blockchain platform is developed and experimentally evaluated. Authentication and authorization of Internet of Things (IoT) devices for conditional data access control are two critical issues. An important conditional data access scenario consists of the following: A device is initialized at the very beginning of its life cycle and should work without updates during its entire life cycle. One version of Broadcast encryption (BE) has been developed to provide conditional data access in the scenario where an entity should be provided with certain credentials during the initialization phase and these cannot be updated during the entire life cycle. Illustrative initial applications were the following ones: a DVD player that provides conditional access to many different DVDs, or a satellite TV broadcasting system that provides conditional access to TV programs based on “pay-per-view” concept, see [1], for example. The traditional paradigm of conditional data access control employing BE is the following one: (i) encrypt data with a session secret key, (ii) append to the encrypted data as a header encrypted version of the current session key encrypted with a number of different keys so that each legitimate user can decrypt the session key and the data, (iii) make the header and the encrypted data publicly available. In particular, BE provides an opportunity for dynamic updates of the access privileges and a high reduction of the header overhead when large clusters of users should obtain the access rights or should be revoked from the set of eligible users. [3]

Saraiva et. al. states that With the growing number of heterogeneous resource-constrained devices connected to the Internet, it becomes increasingly challenging to secure the privacy and protection of data. Strong but efficient cryptography solutions must be employed to deal with this problem, along with methods to standardize secure communications between these devices. The PRISEC module of the UbiPri middleware has this goal. In this work, we present the performance of the AES (Advanced Encryption Standard), RC6 (Rivest Cipher 6), Twofish, SPECK128, LEA, and ChaCha20-

Poly1305 algorithms in Internet of Things (IoT) devices, measuring their execution times, throughput, and power consumption, with the main goal of determining which symmetric key ciphers are best to be applied in PRISEC. We verify that ChaCha20-Poly1305 is a very good option for resource constrained devices, along with the lightweight block ciphers SPECK128 and LEA. With the rapid growth of the IoT (Internet of Things), more devices are connected to the Internet, resulting in bigger data exchanges. In turn, this generates more security and privacy risks for the users of these devices, which is currently one of the biggest challenges of the IoT. Another problem comes from the fact that IoT devices are often limited in terms of computing power, energy, and memory capacity. The standard Internet protocols and cryptography algorithms require many of these resources, which can potentially make them unsuitable for IoT devices. To deal with these problems, lightweight block ciphers can be used to protect data. There is also a lack of standards for heterogeneous technologies and limited resource environments, which is the case of IoT devices. This opens further privacy risks and makes the IoT especially vulnerable to DDoS (distributed denial of service) attacks. [4]

III. Proposed System

The proposed system introduces a secure IoT communication framework for distributed systems using Adaptive Symmetric Key Encryption (ASKE). The primary objective is to ensure confidentiality, integrity, and efficiency of data transmission while adapting dynamically to the constraints of IoT environments such as limited resources, varying network conditions, and diverse device capabilities.

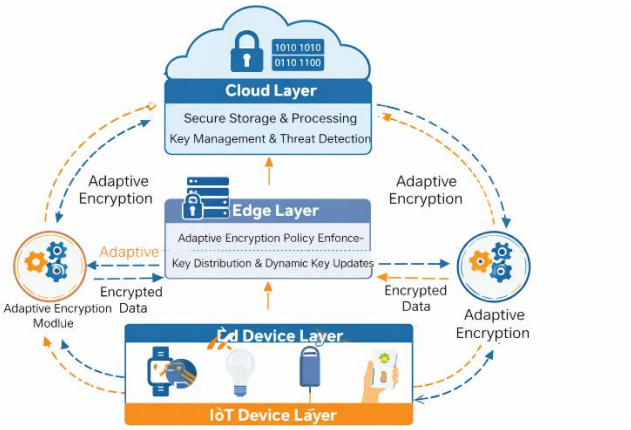

Fig. 1 Secure IoT Communication using Adaptive Symmetric Key encryption

A. System Overview

The system is designed as a multi-layer distributed architecture consisting of IoT devices, edge nodes, and cloud servers. IoT devices collect real-time data and transmit it securely through edge gateways to the cloud. The proposed framework integrates adaptive encryption, intelligent key management, and secure communication protocols to optimize performance and security.

Unlike traditional static encryption methods, the proposed system dynamically adjusts:

- Encryption strength (key size)
- Encryption algorithm selection
- Key refresh rate

based on contextual parameters such as:

- Device energy level
- Network bandwidth
- Data sensitivity
- Threat level

B. Architecture Components

1. IoT Device Layer

This layer consists of resource-constrained devices such as sensors and smart devices. These devices:

- Collect environmental or system data
- Perform lightweight preprocessing
- Apply adaptive symmetric encryption before transmission

Due to limited computational resources, lightweight encryption techniques such as AES (Advanced Encryption Standard - lightweight mode) or ChaCha20 are utilized.

2. Edge Layer (Gateway/Edge Node)

The edge layer acts as an intermediate processing unit between IoT devices and the cloud. Its functions include:

- Device authentication
- Data aggregation and filtering
- Dynamic encryption policy enforcement
- Temporary key management

The edge node plays a critical role in reducing latency and enabling real-time decision-making for adaptive encryption.

3. Cloud Layer

The cloud layer is responsible for:

- Secure storage of encrypted data
- Advanced analytics and processing
- Long-term key management
- Threat detection and monitoring

It also provides scalability and centralized control over the distributed system.

C. Adaptive Symmetric Key Encryption Mechanism

The core of the proposed system is the adaptive encryption module, which dynamically selects encryption parameters.

Working Principle:

1. Data is classified based on sensitivity (Low, Medium, High)
2. System monitors:
   - CPU usage
   - Battery level
   - Network latency

D. Key Management Strategy

Efficient key management is essential in distributed IoT systems. The proposed system uses a hybrid adaptive key management approach:

- Initial Key Generation: Keys are generated using a secure random function at the edge layer
- Key Distribution: Secure channels (TLS-based) are used for key exchange
- Dynamic Key Update: Keys are periodically refreshed based on:
  - Time interval
  - Data volume
  - Detected threats
- Session-Based Keys: Temporary session keys are used to enhance security

E. Security Features

The proposed system ensures protection against common IoT threats:

- Confidentiality: Data is encrypted using adaptive symmetric keys
- Integrity: Hash-based verification ensures data is not altered
- Authentication: Devices are verified before communication
- Attack Prevention:
  - Replay attack protection using timestamps
  - Man-in-the-middle attack mitigation via secure key exchange
  - Data tampering detection using hash validation

IV. Research Methodology

The proposed methodology focuses on designing and evaluating a secure IoT communication system using Adaptive Symmetric Key Encryption (ASKE) in a distributed environment. The system is implemented using a layered architecture consisting of IoT devices, edge nodes, and cloud servers.

A. Methodology Overview

The methodology follows these major steps:

- Data Collection: IoT devices collect real-time data (sensor/environmental data)
- Data Classification
- Data is categorized into:
  - Low sensitivity
  - Medium sensitivity
  - High sensitivity
- System Monitoring
- Continuously monitors:
  - Device energy level

- Network bandwidth
- Latency
- Threat level
- Adaptive Encryption Selection
- Based on monitored parameters:
- Select encryption algorithm (AES / ChaCha20)
- Adjust key size (128-bit / 192-bit / 256-bit)
- Data Encryption & Transmission
- Data is encrypted using symmetric key
- Sent securely to edge node
- Edge Processing
- Authentication
- Key distribution
- Data aggregation
- Cloud Processing
- Secure storage
- Decryption (if required)
- Threat analysis

B. Algorithm (Adaptive Symmetric Key Encryption)

Algorithm 1: ASKE-Based Secure Communication

Input: Data D, Device Status S, Network Status N

Output: Encrypted Data ED

Step 1: Initialize system parameters

Step 2: Capture data D from IoT device

Step 3: Classify data sensitivity level L

if D is critical → L = High

else if moderate → L = Medium

else → L = Low

Step 4: Monitor system parameters:

Energy E ← device battery level

Bandwidth B ← network condition

Threat T ← security level

Step 5: Select encryption parameters:

if L = High or T is High:

Key size = 256-bit

Algorithm = AES

else if E is Low or B is Low:

Key size = 128-bit

Algorithm = ChaCha20

else:

Key size = 192-bit

Algorithm = AES

Step 6: Generate symmetric key K

Step 7: Encrypt data:

ED = Encrypt(D, K)

Step 8: Transmit ED to Edge Layer

Step 9: Edge performs authentication & key update

Step 10: Store/process data in Cloud

End

C. Flowchart (Textual Representation)

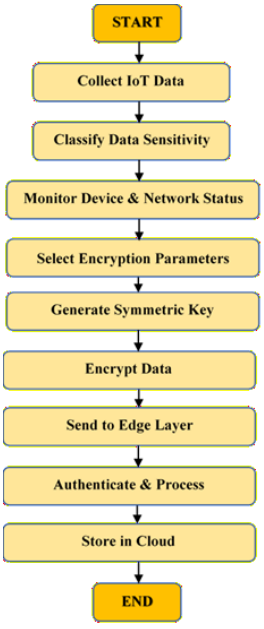

Fig. 2 Flowchart of the proposed system

V. Result And Discussion

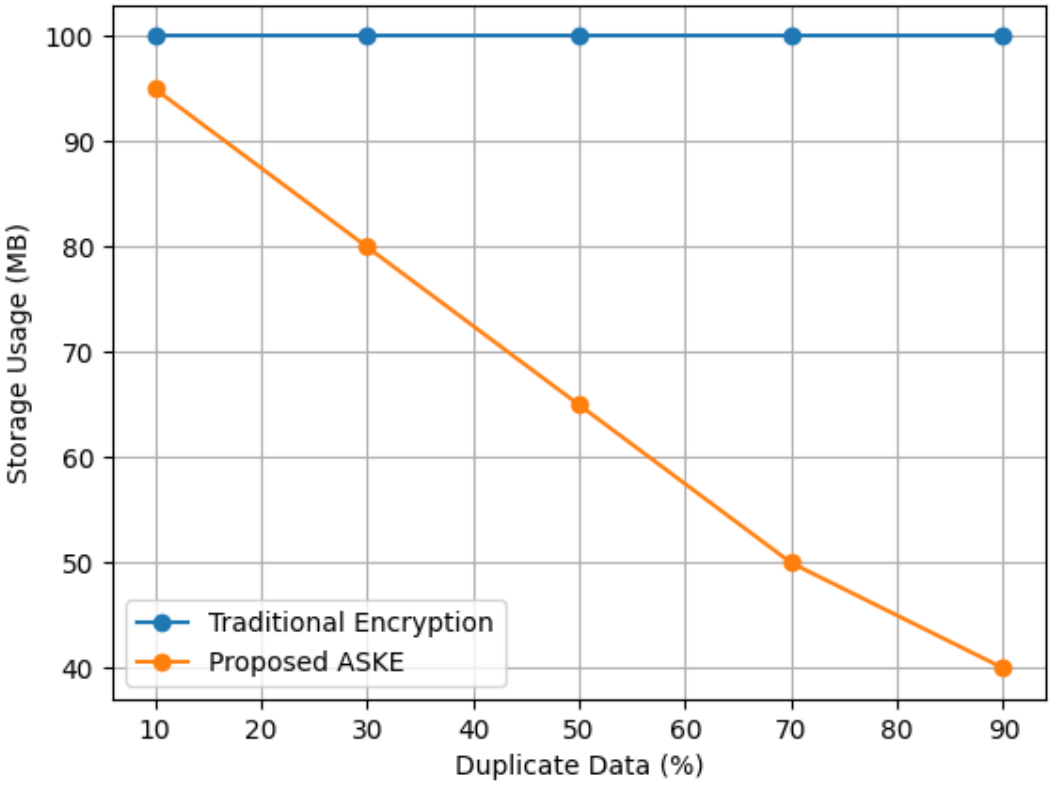

Fig. 3 Storage Efficiency

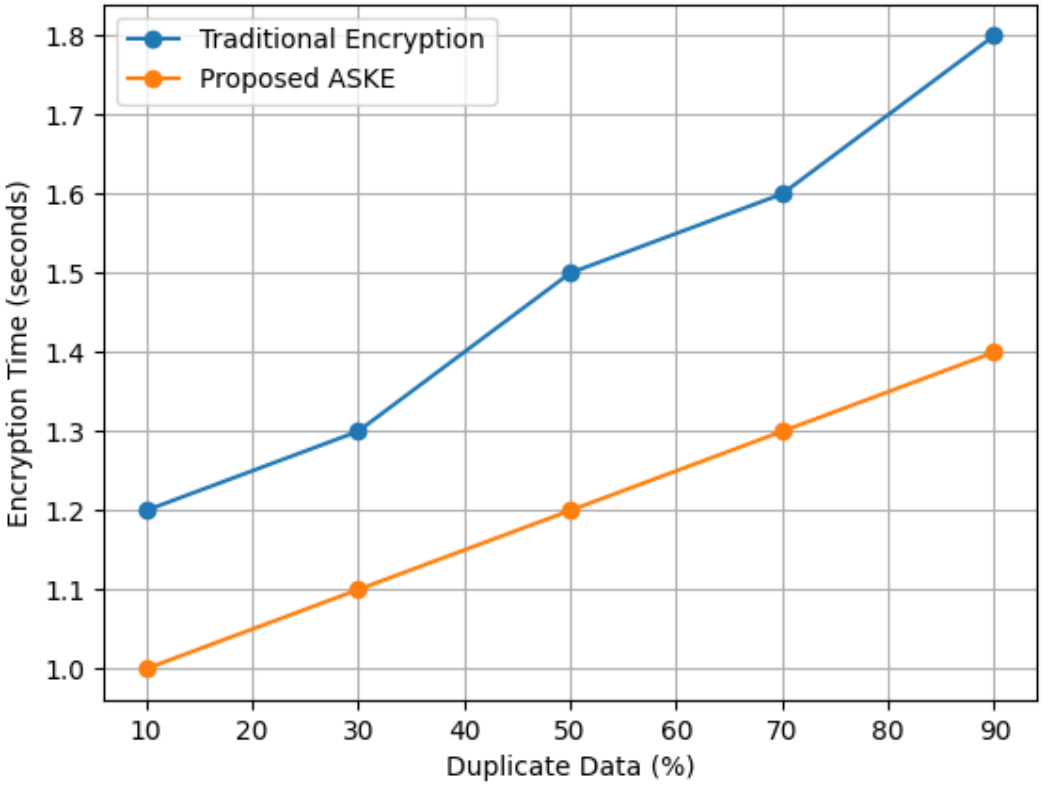

Fig. 4 Encryption Time

VI. Conclusion

Within the scope of this study work, Adaptive Symmetric Key Encryption (ASKE) was proposed as a communication architecture that is not only safe but also effective for Internet of Things (IoT) devices that are spread around the globe. Systems that are connected to the Internet of Things are typically confronted with a number of important challenges. These challenges can be broken down significantly. The constraints on the resources that are available, worries regarding the safety of the data, and the ever-changing conditions of the network are all examples of these problems. The approach that has been presented is one that addresses the challenges that have been outlined beforehand. This method makes dynamic modifications to encryption parameters such as key size and algorithm based on real-time factors such as the sensitivity of the data, the capability of the device, the capacity of the network, and the level of threat. Traditional encryption methods are based on static configurations, but the method that has been suggested makes these modifications dynamically. In contrast to this, the conventional encryption systems, which are founded on static setups, are based on dynamic configurations. For the goal of ensuring that dispersed systems and the Internet of Things are able to communicate in a secure manner, the ASKE-based architecture that has been outlined provides a solution that is not only long-lasting but also scalable and lightweight. In conclusion, this design has been described in detail. It is possible that in the future, the primary focus of research will be on the application of machine learning algorithms for predictive threat detection, the improvement of blockchain-based key management, and the testing of the system in actual Internet of Things circumstances. All of these are additional methods that can be utilized to enhance the system's capabilities in terms of reliability and security.

References

[1] D. Shivaramakrishna, M. Nagaratna, “A novel hybrid cryptographic framework for secure data storage in cloud computing: Integrating AES-OTP and RSA with adaptive key management and Time-Limited access control”, Alexandria Engineering Journal 84 (2023) 275–284

[2] Yuan Cheng, Yanan Liu, Zheng Zhang and Yanxiu Li, “An Asymmetric Encryption-Based Key Distribution Method for Wireless Sensor Networks”, Sensors 2023, 23, 6460

[3] Miodrag J. Mihaljevi´c, Milica Kneževi´c, Dragan Uroševi´c, Lianhai Wang, Shujiang Xu, “An Approach for Blockchain and Symmetric Keys Broadcast Encryption Based Access Control in IoT”, Symmetry 2023, 15, 299

[4] Daniel A. F. Saraiva, Valderi Reis Quietinho Leithardt, Diandre de Paula, André Sales Mendes, Gabriel Villarrubia González, Paul Crocker, “PRISEC: Comparison of Symmetric Key Algorithms for IoT Devices”, Sensors 2019, 19, 4312

[5] Umer Farooq, Najam Ul Hasan, Imran Baig, Naeem Shehzad, “Efficient adaptive framework for securing the Internet of Things devices”, URASIP Journal on Wireless Communications and Networking (2019) 2019:210

[6] Department of Information Technology, KLN College of Engineering, Madurai, India, G. Ramesh, J. Logeshwaran, Department of ECE, Sri Eshwar College of Engineering, Coimbatore, India, V. Aravindarajan, and Department of Information Technology, KLN College of Engineering, Madurai, India, “A Secured Database Monitoring Method to Improve Data Backup and Recovery Operations in Cloud Computing,” BIJCS, vol. 2, no. 1, pp. 1–7, 2023, doi: 10.54646/bijcs.019.

[7] “Secure Machine Learning Scenario from Big Data in Cloud Computing via Internet of Things Network | SpringerLink.” Accessed: Aug. 27, 2023. [Online].

[8] S. Shakya, An efficient security framework for data migration in a cloud computing environment, JAICN 01 (01) (2019) 45–53, https://doi.org/10.36548/ jaicn.2019.1.006.

[9] Z. Wang, N. Wang, X. Su, S. Ge, An empirical study on business analytics affordances enhancing the management of cloud computing data security, Int. J. Inf. Manag. 50 (2020) 387–394

[10] H. Qiu, M. Qiu, M. Liu, G. Memmi, Secure Health Data Sharing for Medical CyberPhysical Systems for the Healthcare 4.0, IEEE J. Biomed. Health Inform. 24 (9) (2020) 2499–2505

[11] P. Wei, D. Wang, Y. Zhao, S.K.S. Tyagi, N. Kumar, Blockchain data-based cloud data integrity protection mechanism, Futur. Gener. Comput. Syst. 102 (2020) 902–911

[12] G.S. Aujla, A. Singh, M. Singh, S. Sharma, N. Kumar, K.-K.-R. Choo, BloCkEd: blockchain-based secure data processing framework in edge envisioned V2X environment, IEEE Trans. Veh. Technol. 69 (6) (2020) 5850–5863

[13] C. Feng, et al., Efficient and secure data sharing for 5G flying drones: A blockchainenabled approach, IEEE Netw. 35 (1) (2021) 130–137, https://doi.org/10.1109/ MNET.011.2000223.

[14] "Sustainability | Free Full-Text | A Secure Data Sharing Platform Using Blockchain and Interplanetary File System." Accessed: Aug. 27, 2023. [Online]. Available: htt ps://www.mdpi.com/2071-1050/11/24/7054.

[15] "Enhancing the security of cloud data using hybrid encryption algorithm | SpringerLink." Accessed: Aug. 27, 2023. [Online]. Available: https://link.springer. com/article/10.1007/s12652-019-01403-1